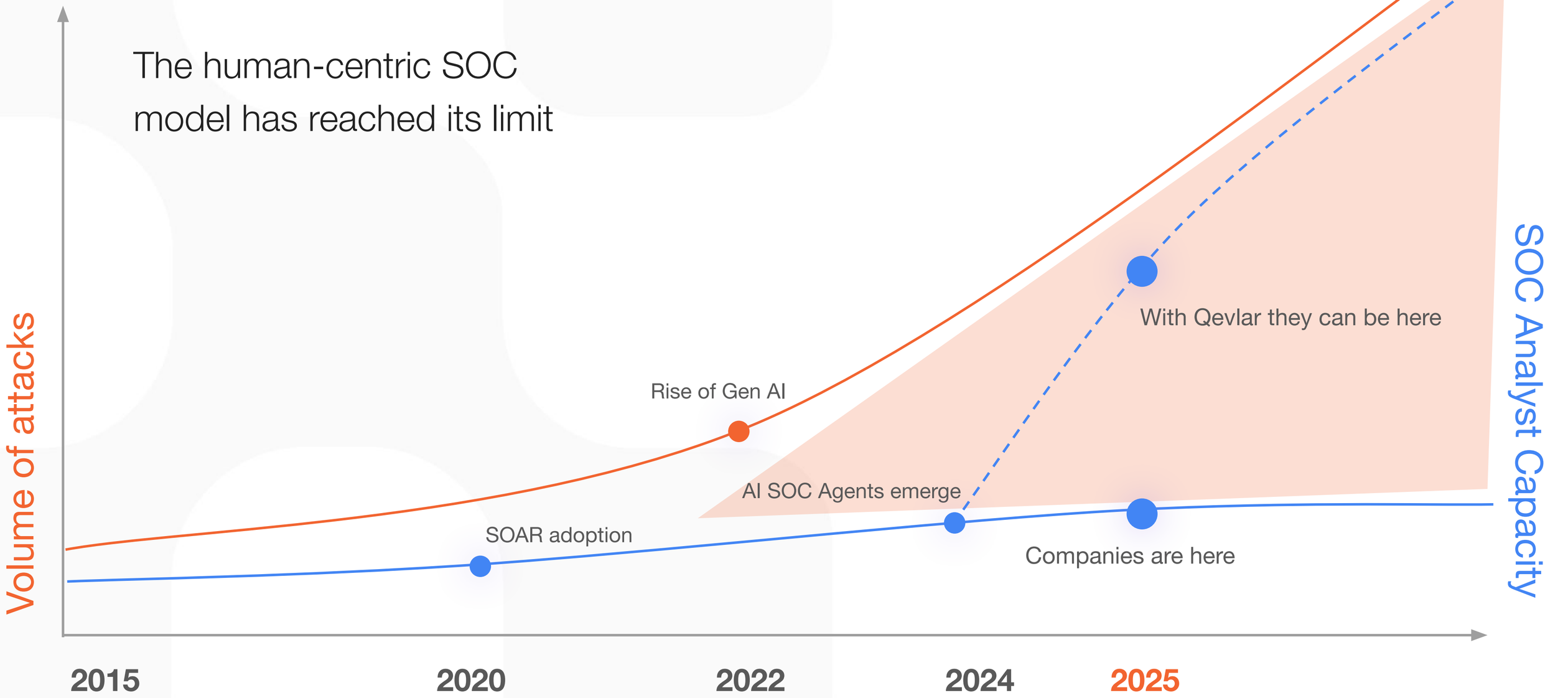
The AI SOC platform that doesn't hallucinate

Qevlar AI

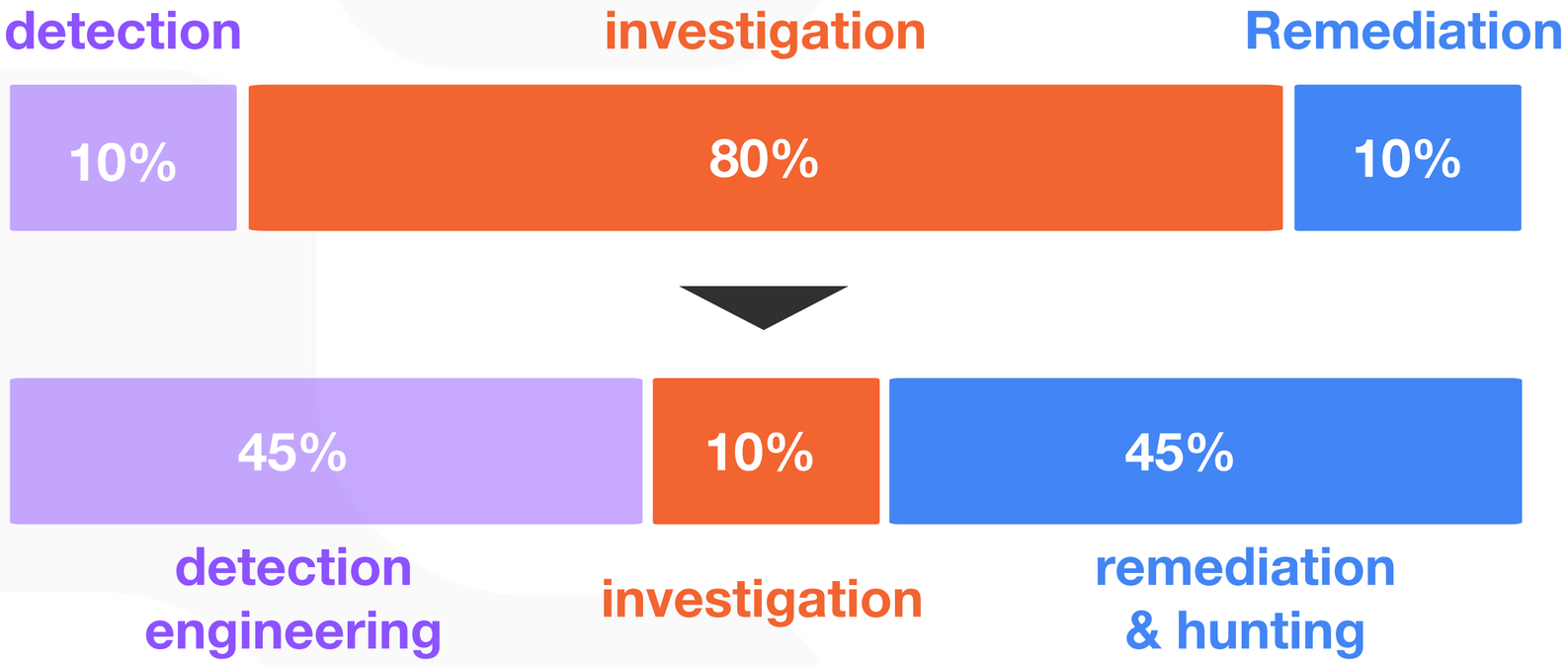
almond Atos GLOBAL CONNECT BOUYGUES Mercedes Benz stoïk sodexo nomios Orange Cyberdefense

The SOC Capacity **Gap**

The human-centric SOC model has reached its limit

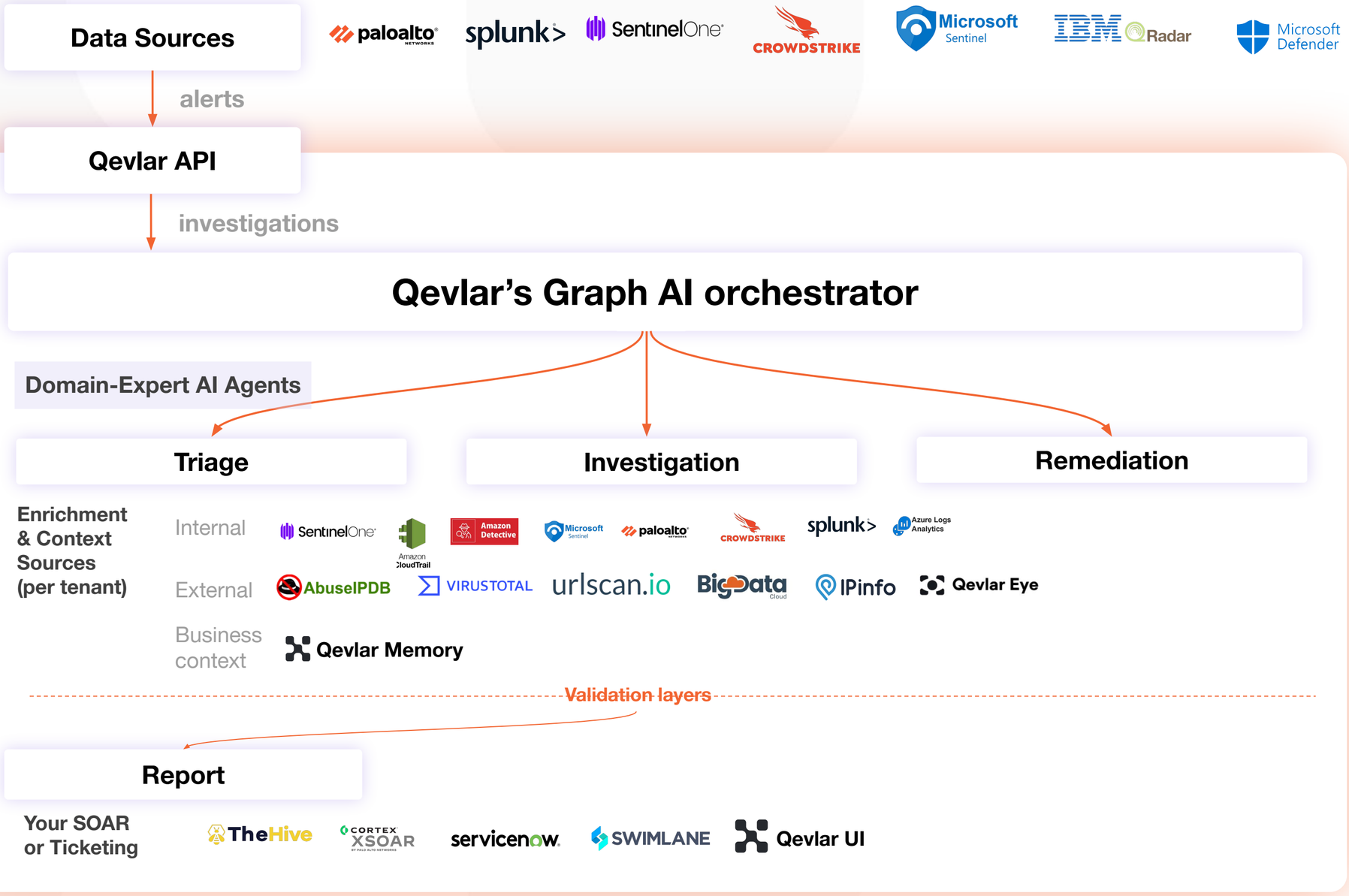


AI SOC analysts to unlock real time SOC



We take most analysts' tasks off, **freeing them to tackle high-impact challenges.**

Qevlar works in your SOC environment



Deployment is **within a few hours** via API: SaaS or BYOC

Graph AI orchestrator **stabilizes LLMs** for consistent results: it breaks investigation into micro-tasks for LLMs and validates outputs

Supports **multi-tenancy**: client data is isolated from each other

Every conclusion is **based on facts and evidence**, so you can trace its reasoning transparently

Qevlar runs **headlessly**, enriching your existing tools without adding another console

State of alert investigation at SOCs

	Average SOC	With Qevlar
Average investigation time	30’	3’
On 25,000 alerts	12,500 hours or ~6.2 years of full-time work for one analyst	1,250 hours or ~156 working days
Time spent on false threats	~80%	0%

90%
Reduced investigation time

6 years
of full-time analyst work can be refocused on higher-value tasks

~80%
tickets are ready to be closed

Qevlar AI **10x the efficiency** of SOCs



Farah Rigal

Deputy Head of Cybersecurity Services

Atos

*"Our focus is on taking the **AI opportunity for higher predictability**, actionability and efficiency while managing its inherent risks."*



Julio Garcia

Cyber Defense Hub Lead

*"Working with Qevlar AI It is like you **change** from a regular car to a **sports car.**"*



Frédéric Zink

Managing Director

orange Cyberdefense

*"We can now detect threats **more quickly and accurately**, while focusing our analysts' expertise on the most complex and critical incidents."*